

27. 1. 2004

日本国特許庁
JAPAN PATENT OFFICE

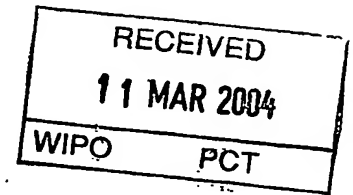
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 2月26日

出願番号
Application Number: 特願2003-049710
[ST. 10/C]: [JP 2003-049710]

出願人
Applicant(s): 松下電器産業株式会社

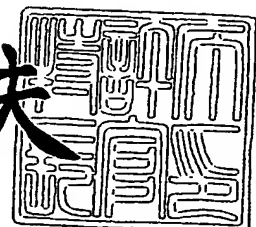


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2004年 2月27日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



【書類名】 特許願
【整理番号】 2032750014
【あて先】 特許庁長官殿
【国際特許分類】 G06F 9/06

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 三浦 康史

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 徳田 克己

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 山本 雅哉

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【電話番号】 06-4806-7530

【手数料の表示】

【予納台帳番号】 049515

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213583

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルコンテンツ配信システム

【特許請求の範囲】

【請求項 1】 ユーザにコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とから構成されるデジタルコンテンツ配信システムであって、

前記サーバ装置および前記端末装置は、少なくともトランザクション識別ビットを記憶するトランザクション識別ビット記憶手段を持つことにより、

複数トランザクション処理を行う場合において、前記サーバ装置と前記端末装置間の通信往復回数および前記サーバ装置と前記端末装置で管理する情報量が少ない通信を行うことを特徴とするコンテンツ配信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークを用いて、サーバ装置から映像、音楽などのデジタルコンテンツと、デジタルコンテンツの利用を許諾するライセンスを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、前記サーバ装置と前記端末装置間の通信において、不正にライセンスの複製や改ざんが行われることを防ぎつつ、通信切断発生時においてもライセンスの消失や二重配信をも防ぐシステムおよび装置に関する。

【0002】

【従来の技術】

近年、音楽、映像、ゲーム等のデジタルコンテンツ（以下、コンテンツと記述）を、インターネット等の通信やデジタル放送等を通じて、サーバ装置から端末装置に配信し、端末装置においてコンテンツを利用することが可能な、コンテンツ配信システムと呼ばれるシステムが実用化段階に入っている。一般的なコンテンツ配信システムでは、コンテンツの著作権を保護し、悪意あるユーザ等によるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保

護技術とは、具体的には、暗号技術等を用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。

【0003】

例えば、特許文献1には、コンテンツ配信システムの一例として、暗号化されたコンテンツ、利用条件、および、コンテンツ復号鍵を端末装置が、サーバ装置より受信し、改ざん検出を行った後、利用条件の適合検証を行い、すべての検証を満足したときのみコンテンツの復号を行い出力するシステムが記載されている。

【0004】

このように、従来のコンテンツ配信システムでは、サーバ装置からライセンス（利用条件とコンテンツ復号鍵の総称。利用権利とも呼ぶ）を端末装置に配信するが、その配信経路は一般的にインターネットなどの公衆回線を用いるため、ライセンスの盗聴および改ざんを防ぐ必要がある。つまり、利用条件の不正改ざんやコンテンツ鍵の流出を防止しなければならない。さらに、サーバ装置はライセンス配信先の認証も行う必要がある。つまり、サーバ装置が意図しない端末装置にライセンスを配信することも防止する必要がある。盗聴・改ざん防止と通信相手の認証を行うプロトコルはSAC（Secure Authenticated Channel）プロトコルと呼ばれ、例えば、SSL（Secure Socket Layer）がよく知られている（非特許文献1）。

【0005】

また、通信装置・通信回線の故障や電源断などによる通信切断がライセンス配信中に発生した場合、そのライセンスが消失してしまう可能性がある。このような場合、購入したコンテンツを再生することができないといった不利益がユーザに発生する。例えば、特許文献2および特許文献3には、通信切断による通信データの消失を、データ再送によって回避するプロトコルが記載されている。

【0006】

【特許文献1】

特許第3276021号公報

【0007】

【特許文献2】

特開 2002-251524 号公報

【0008】

【特許文献3】

特開 2003-16041 号公報

【0009】

【非特許文献1】

A.Frier, P.Karlton, and P.Kocher, "The SSL 3.0 Protocol", [online], NetScape Communications Corp., Nov. 18, 1996, [平成15年1月17日検索], インターネット<URL: <http://wp.netscape.com/eng/ssl3/draft302.txt>>

【0010】

【発明が解決しようとする課題】

しかしながら、SACプロトコルや通信切断対策プロトコルは、その適用範囲を広げるために汎用性を重視し、それぞれ独立に提案されている。これにより、双方のプロトコルを利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となる。

【0011】

また、ライセンス取得やライセンス返却などのトランザクションを連続して行う場合、トランザクション毎にSACプロトコルと通信切断対策プロトコルを単純に繰り返すことにすれば、1回のトランザクション処理にかかる通信往復回数の倍数だけ通信往復回数が増えていくこととなる。例えば、1回のトランザクション処理にかかる通信往復回数を4回とする場合、 n 個のトランザクションを処理する際には $4n$ 回の通信往復回数が必要となる。

【0012】

それゆえ、端末装置がトランザクション処理を完了するまでに通信遅延が発生し、ユーザが要求を出してから、応答を得るまでに待ち時間が発生するという課題があった。

【0013】

本発明は、こうした従来の問題点を解決するものであり、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、複数トランザクション処理を行う場合において、サーバ装置・端末装置間の通信往復回数を減少させ、さらに、上記機能を実現するためにサーバ装置と端末装置で管理・保持する情報が少ないプロトコルを実現するシステムおよび装置を提供する。これにより、ユーザが要求を出してから、応答を得るまでの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することを目的としている。

【0014】

本発明のプロトコルを利用した場合、 n 個のトランザクションを処理する際の通信往復回数は $n + 2$ となる。

【0015】

【課題を解決するための手段】

上記目的を達成するために、本発明に関わるコンテンツ配信システムは、ユーザにコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とから構成されるデジタルコンテンツ配信システムであって、前記サーバ装置および前記端末装置は、少なくともトランザクション識別ビットを記憶するトランザクション識別ビット記憶手段を持つことにより、複数トランザクション処理を行う場合において、ユーザに対する応答時間を削減することを特徴とする。

【0016】

【発明の実施の形態】

(実施の形態 1)

図 1 は、本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図である。図 1 において、本発明の一実施形態に係るコンテンツ配信システムは、サービス提供者側であるコンテンツ配信装置 1 と利用者側であるユーザ端末 3 とが、ネットワーク等の伝送路で接続される構成である。

【0017】

コンテンツ配信装置 1 は、コンテンツ購入処理部 11 と、ユーザ登録部 12 と、ユーザ権利登録部 13 と、ユーザ権利作成部 14 と、コンテンツ暗号化部 15 と、コンテンツ管理部 16 と、セキュリティ管理／通信部 17 と、ユーザデータベース 18 と、コンテンツ権利データベース 19 と、ユーザ所有権利データベース 20 と、コンテンツデータベース 21 とを備えている。また、ユーザ端末 3 は、ユーザ指示処理部 31 と、端末情報記憶部 32 と、コンテンツ蓄積部 33 と、利用権利管理部 34 と、利用権利データベース 35 と、セキュリティ管理／通信部 36 と、出力部 37 とを備えている。

【0018】

まず、上記コンテンツ配信システムを構成するコンテンツ配信装置 1 およびユーザ端末 3 の概要を、以下に説明する。

コンテンツ配信装置 1 において、コンテンツ購入処理部 11 は、コンテンツ購入処理実行時に、コンテンツ権利データベース 19 に格納されている各コンテンツの内容、利用条件および料金等の情報を、ユーザ端末 3 へ送信してユーザに提示する。また、コンテンツ購入処理部 11 は、ユーザによってコンテンツが購入された場合には、ユーザ端末 3 からユーザ情報（ユーザ ID、端末 ID、ユーザ名、電話番号等）を取得すると共に、必要な課金処理を行う。コンテンツ権利データベース 19 には、コンテンツ（映画や TV 放送等の動画、書籍や印刷物等の静止画、ラジオ放送や朗読等の音声および音楽、ゲーム等）毎に、コンテンツ利用に関する 1 つ又は複数の情報が格納されている。

【0019】

ユーザ登録部 12 は、コンテンツ購入処理部 11 で取得されたユーザ情報を、ユーザデータベース 18 に記憶して登録する。ユーザデータベース 18 には、コンテンツ購入を行ったユーザの情報が、累積的に記憶されている。

【0020】

ユーザ権利登録部 13 は、ユーザ登録部 12 を介してコンテンツ購入処理部 11 から与えられる、ユーザが購入したコンテンツに関する情報を、ユーザが所有する権利としてユーザ所有権利データベース 20 に記憶して登録する。ユーザ所

有権利データベース 20 には、ユーザが購入したコンテンツの利用権利が記憶されている。

【0021】

ユーザ権利作成部 14 は、ユーザ端末 3 から受けるコンテンツ利用要求に応じて、ユーザ端末 3 へ送信する利用権利（利用条件、コンテンツの復号鍵）を生成する。

【0022】

コンテンツ暗号化部 15 は、ユーザ端末 3 へ送信するコンテンツの暗号化を行い、コンテンツデータベース 21 へ暗号化コンテンツの登録を行う。

コンテンツ管理部 16 は、ユーザ端末 3 へ送信する暗号化コンテンツをコンテンツデータベース 21 から検索し、セキュリティ管理／通信部 17 へ渡す。

【0023】

セキュリティ管理／通信部 17 は、ユーザ端末 3 の認証、コンテンツ配信装置 1 とユーザ端末 3 との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部 17 の構成および通信プロトコルの詳細については後述する。

【0024】

ユーザ端末 3 において、ユーザ指示処理部 31 は、ユーザが入力する指示（コンテンツ購入要求やコンテンツ利用要求等の指示）を処理する。

端末情報記憶部 32 には、上述したユーザ情報（ユーザ ID、端末 ID、ユーザ名、電話番号等）が記憶されている。

【0025】

コンテンツ蓄積部 33 には、購入によって取得された暗号化コンテンツが蓄積される。

利用権利管理部 34 は、コンテンツ利用要求に応答してコンテンツ配信装置 1 から送信されてくる利用権利を受信し、その内容に従って、対応するコンテンツの処理（暗号解読や利用条件に基づく再生等）を実行する。この利用権利は、利用権利データベース 35 に格納されて管理される。

【0026】

出力部 37 は、例えばディスプレイ等の表示装置であって、利用権利管理部 34 が実行する処理に応じてコンテンツの出力を行う。

セキュリティ管理／通信部 36 は、コンテンツ配信装置 1 の認証、コンテンツ配信装置 1 とユーザ端末 3 との間の秘匿通信（盗聴・改ざんの防止と通信相手の認証を行う通信）、および通信切断対策を行う。セキュリティ管理／通信部 36 の構成および通信プロトコルの詳細については後述する。

【0027】

次に、コンテンツ配信装置 1 におけるセキュリティ管理／通信部 17 の構成の詳細について図 2 を用いて説明する。固有鍵情報記憶部 201 は、公開鍵暗号方式におけるコンテンツ配信装置 1 固有の公開鍵 KD_s が含まれるサーバ公開鍵証明書と、コンテンツ配信装置 1 固有の秘密鍵 KE_s と、認証局公開鍵証明書とを記憶する。サーバ公開鍵証明書はコンテンツ配信装置 1 の公開鍵 KD_s に認証局の署名が施されたものである。公開鍵証明書のフォーマットには、一般的な X.509 証明書フォーマットを用いるものとする。公開鍵暗号方式および X.509 証明書フォーマットについては、ITU-T 文書 X.509 “The Directory: Public-key and attribute certificate frameworks” が詳しい。

【0028】

乱数発生部 202 は、乱数の生成を行う。生成された乱数は制御部 204 へ渡される。

暗号処理部 203 は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。データの暗号化および復号アルゴリズムには AES (Advanced Encryption Standard) を、署名生成および署名検証アルゴリズムには ECDSA (Elliptic Curve Digital Signature Algorithm) を用いる。AES については National Institute Standard and Technology (NIST)、FIPS Publication 197、ECDSA については IEEE 1363 Standard が詳しい。

【0029】

暗号処理部203は、データの暗号化／復号を行う場合には、AES鍵と平文／暗号化データをそれぞれ入力とし、入力されたAES鍵で暗号化／復号したデータをそれぞれ出力する。また、署名生成／検証を行う場合には、署名対象データ／署名検証データと秘密鍵／公開鍵をそれぞれ入力とし、署名データ／検証結果をそれぞれ出力する。さらに、セッション鍵生成用パラメータの生成を行う場合には、乱数を入力とし、Diffie-Hellmanパラメータを出力する。また、セッション鍵の生成を行う場合、乱数とDiffie-Hellmanパラメータを入力とし、セッション鍵を出力する。ここで、セッション鍵の生成にはECDH (Elliptic Curve Diffie-Hellman) を用いる。ECDHのアルゴリズムは、上記のIEEE 1363 Standardが詳しい。

【0030】

制御部204は、ユーザ端末3の認証処理、ユーザ端末3と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部204は、トランザクションに1ビットのトランザクション識別ビットを割り当て、そのトランザクション識別ビットと通信ステップ情報を通信ログデータベース206に保存することにより、通信切断対策処理を行う。ここで、トランザクションとは、「利用権利の取得」や「利用権利の返却」などの処理単位を表す。

通信部205は、ユーザ端末3のセキュリティ管理／通信部36と通信を行う。

【0031】

次に、ユーザ端末3におけるセキュリティ管理／通信部36の構成の詳細について図3を用いて説明する。固有鍵情報記憶部301は、公開鍵暗号方式におけるユーザ端末3固有の公開鍵KDcが含まれる端末公開鍵証明書と、ユーザ端末3固有の秘密鍵KEcと、認証局公開鍵証明書を記憶する。端末公開鍵証明書はユーザ端末3の公開鍵KDcに認証局の署名が施されたものである。公開鍵証明書のフォーマットには、コンテンツ配信装置1と同様にX.509証明書フォーマットを用いる。

【0 0 3 2】

乱数発生部 3 0 2 は、乱数の生成を行う。生成された乱数は制御部 3 0 4 へ渡される。

暗号処理部 3 0 3 は、データの暗号化、復号、署名生成、署名検証、セッション鍵生成用パラメータの生成、セッション鍵の生成を行う。暗号処理部 3 0 3 の入出力は、コンテンツ配信装置 1 の暗号処理部 2 0 3 と同じである。

【0 0 3 3】

制御部 3 0 4 は、コンテンツ配信装置 1 の認証処理、コンテンツ配信装置 1 と送受信するデータの暗号化／復号、改ざんのチェックを行う。さらに、制御部 3 0 4 は、コンテンツ配信装置 1 が生成したトランザクション識別ビットと通信ステップ情報を通信ログデータベース 3 0 6 に蓄積することにより、通信切断対策処理を行う。

通信部 3 0 5 は、ユーザ端末 3 側のセキュリティ管理／通信部 1 7 と通信を行う。

【0 0 3 4】

次に、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ配信方法を、図 4 ～図 1 2 を参照して具体的に説明する。

【0 0 3 5】

図 4 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入に関する処理を説明するフローチャートである。図 5 は、コンテンツ権利データベース 1 9 に格納されているコンテンツに関する情報の一例を概念的に示す図である。図 6 は、ユーザデータベース 1 8 に格納されているユーザ情報の一例を概念的に示す図である。図 7 は、ユーザ所有権利データベース 2 0 に格納されているユーザが所有する権利の情報の一例を概念的に示す図である。図 8 は、コンテンツデータベース 2 1 に格納されているコンテンツ情報の一例を概念的に示す図である。図 9 は、本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャートである。図 1 0 ～図 1 2 は、本発明の一実施形態に係るコンテンツ配信システムで行われる秘匿通信と通信切断対策処理を説明するフローチャートである。

【0036】**(1) コンテンツ購入処理**

図4を参照して、コンテンツ配信装置1で提供されるコンテンツをユーザが購入する際に、コンテンツ配信システムで行われる処理を説明する。

【0037】

ユーザ端末3では、ユーザが、コンテンツ購入に関する指示をユーザ指示処理部31へ出力する。ユーザ指示処理部31は、セキュリティ管理／通信部36を介して、指示に応じたコンテンツ購入要求をコンテンツ配信装置1へ発行する（ステップS41）。

【0038】

コンテンツ配信装置1では、ユーザ端末3から発行されたコンテンツ購入要求が、セキュリティ管理／通信部17を介してコンテンツ購入処理部11で受信される。コンテンツ購入処理部11は、コンテンツ購入要求を受信すると、コンテンツ権利データベース19から格納されているすべてのコンテンツに関する情報を取得し、セキュリティ管理／通信部17を介してユーザ端末3へ送信する（ステップS42）。

【0039】

ここで、コンテンツ権利データベース19には、例えば図5に示すような情報が格納されている。図5において、コンテンツ名は、コンテンツの名称であり、コンテンツIDは、コンテンツを識別するために付される固有の番号である。利用条件は、通常使用される予め定めたデータ形式によって、コンテンツを利用できる具体的な条件を示すものである。各コンテンツに設定される利用条件および金額は、1つであってもよいし、複数であってもよい。この例では、映画Aというコンテンツには、再生回数による利用条件が設定されており、400円を支払えば、映画Aを2回観賞することができることを表している。

【0040】

なお、利用条件には、上述した利用回数や利用時間以外にも、利用期間、記録媒体へのコピーや書面への印刷の可否等の様々な条件を使用することが可能である。

【0041】

再び図4を参照して、ユーザ端末3において、コンテンツ購入処理部11から送信されたコンテンツに関する情報(図5)が確認され、ユーザがいずれかのコンテンツの購入を決定した場合(ステップS43, Yes)、ユーザ指示処理部31は、コンテンツ購入決定通知(購入したコンテンツおよび選択した利用条件の情報を含む)と共に、端末情報記憶部32に格納されているユーザ情報を、セキュリティ管理/通信部36を介してコンテンツ配信装置1へ送信する(ステップS44)。

【0042】

コンテンツ配信装置1では、ユーザ端末3から送信されるコンテンツ購入決定通知およびユーザ情報を、セキュリティ管理/通信部17を介してコンテンツ購入処理部11で受信する。そして、コンテンツ購入処理部11は、必要な課金処理を実行すると共に、購入されたコンテンツの情報とユーザ情報とを、ユーザ登録部12へ送出する(ステップS45)。なお、課金処理は本発明の主眼ではないので、説明を省略する。

【0043】

ユーザ登録部12は、コンテンツ購入処理部11から送出される購入されたコンテンツの情報およびユーザ情報を、ユーザ権利登録部13へ転送すると共に、ユーザ情報をユーザデータベース18に記憶して登録する(ステップS47)。このとき、コンテンツ購入処理部11から送出されるユーザ情報と同一の内容が、既にユーザデータベース18に登録されている場合には、上述したユーザ登録は行われ(ステップS46, Yes)。

【0044】

ユーザデータベース18には、例えば図6に示すような情報が格納される。図6において、ユーザIDは、ユーザを識別するために付される固有の番号である。ユーザ名は、ユーザの名前である。端末IDは、端末を識別するために付される固有の番号であり、1人のユーザが複数の端末を所有している場合等に利用される。電話番号は、ユーザを特定するために利用される。図6の例では、“ユーザID「0001」である「一朗」というユーザが、ID番号「1234567

」の端末を利用する”という内容が、ユーザ情報として登録されている。

【0045】

ユーザ権利登録部13は、購入によってユーザが所有することになるコンテンツ利用の権利を、ユーザ登録部12から与えられる購入されたコンテンツの情報とユーザ情報とに基づいて、ユーザ所有権利データベース20に記憶して登録する(ステップS48)。

【0046】

ユーザ所有権利データベース20には、例えば図7に示すような情報が格納されている。図7において、ユーザIDは、ユーザデータベース18に登録されている情報である。コンテンツIDおよび利用条件は、コンテンツ権利データベース19に登録されている情報である。

【0047】

上記処理によって、コンテンツの購入およびその購入に伴うユーザの所有権利の登録が完了する。

【0048】

(2) コンテンツ利用処理

次に、図9を参照して、上述した処理によってユーザ所有権利データベース20にユーザ所有権利が登録された後、ユーザが購入したコンテンツを利用する際にコンテンツ配信システムで行われる処理を説明する。

【0049】

ユーザ端末3では、ユーザが、コンテンツ利用に関する指示をユーザ指示処理部31へ出力する。このとき、ユーザは、コンテンツをどのように利用するのかの指示を与える。例えば、購入したコンテンツの利用条件が回数であれば何回利用したいのか、時間であれば何分利用したいのかという指示を与える。ユーザ指示処理部31は、セキュリティ管理／通信部36を介して、指示に応じたコンテンツ利用要求をコンテンツ配信装置1へ送信する(ステップS91)。なお、コンテンツ利用要求は、必ずしもユーザ指示に従って作成されるものではなく、ユーザ端末3内で自動的に作成される場合もある。例えば、端末3がサポートするコンテンツの利用条件が固定されている場合、ユーザが指示を与えるまでもなく

、コンテンツ利用要求をユーザ端末3内で作成することができる。具体的には、ユーザ端末3が、記憶容量の制限により毎回1回分の利用権利だけが取得・処理可能な端末の場合であり、この場合には端末に応じたコンテンツ利用要求をユーザ指示処理部31で自動的に作成し、コンテンツ配信装置1へ発行する。このコンテンツ利用要求には、上記指示の内容、ユーザID、端末IDおよびコンテンツIDが含まれる。

【0050】

コンテンツ配信装置1では、ユーザ端末3から送信されたコンテンツ利用要求を、セキュリティ管理／通信部17を介してユーザ権利作成部14で受信する。ユーザ権利作成部14は、コンテンツ利用要求を受信すると、この要求に対応した内容が登録されているか否かを、ユーザデータベース18およびユーザ所有権利データベース20を参照して確認する（ステップS92）。具体的には、ユーザ権利作成部14は、コンテンツ利用要求に含まれるユーザIDおよび端末IDが、ユーザデータベース18に登録されているか否かをまず確認し、登録されていると判断すると、そのユーザIDにおいてコンテンツ利用要求に含まれるコンテンツIDおよび指示に応じた利用条件が、ユーザ所有権利データベース20に登録されているか否かを確認する。

【0051】

上記ステップS92における確認の結果、コンテンツ利用要求に対応した内容が登録されていると判断した場合（ステップS93, Yes）、ユーザ権利作成部14は、コンテンツ利用要求に応じた利用権利を作成し、セキュリティ管理／通信部17を介してユーザ端末3へ送信する（ステップS94）。また、ユーザ権利作成部14は、コンテンツ利用要求に含まれるコンテンツIDをコンテンツ管理部16へ通知する。コンテンツ管理部16は、コンテンツIDに対応するコンテンツをコンテンツデータベース21から取り出し、セキュリティ管理／通信部17を介してユーザ端末3へ送信する（ステップS95）。

【0052】

一方、上記ステップS92における確認の結果、コンテンツ利用要求に対応した内容が登録されていないと判断した場合（ステップS93, No）、ユーザ権

利作成部 14 は、コンテンツ利用要求を拒絶する旨を、セキュリティ管理／通信部 17 を介してユーザ端末 3 へ通知する（ステップ S 97）。

【0053】

ここで、上記ステップ S 94 で行われる利用権利の生成は、次のようにして行われる。前提として、ユーザ ID「0001」のユーザが、図 7 のユーザ所有権利データベース 20 に示される登録内容で、事前にコンテンツの購入を行っていたと仮定する。

【0054】

さらに、そのユーザが、コンテンツ ID「112233」のコンテンツを 1 回利用したいというコンテンツ利用要求を送信してきた場合を考える。この場合、ユーザ所有権利データベース 20 に登録されている利用条件が 2 回であるので、ユーザ権利作成部 14 は、要求通り再生回数＝1 を与える情報および該当コンテンツの復号鍵を含む利用権利を作成する。また、ユーザ権利作成部 14 は、この利用権利の作成と同時に、ユーザ所有権利データベース 20 に登録されている利用条件の回数を 1 つ減少させて、登録内容を更新する（図 7 の例では、2→1）。ただし、通信切断対策処理において、セキュリティ管理／通信部 17 から再開トランザクションとして指示された場合には、登録内容の更新を行わない。なお、通信切断対策処理については後述する。

【0055】

なお、ユーザ権利作成部 14 は、通信切断対策処理により再開トランザクションが発行されることを想定して、作成したユーザ権利を保存しておいてもよい。これにより、再開トランザクション発行時にユーザ権利を再度作成する手間を省くことができる。

【0056】

なお、ユーザ端末 3 へ利用権利を発行する毎に、ユーザ所有権利データベース 20 に登録されている内容を更新した結果、コンテンツの購入によって与えられた利用条件がなくなった場合には、ユーザ所有権利データベース 20 に登録されている該当ユーザ所有権利を削除してもよいし、そのまま残しておいてもよい。残しておく場合には、同一のユーザが再度同じコンテンツの購入を行ったときや

、ユーザが取得した利用権利を行使せずに返却するとき等に、処理対応がしやすくなる。

【0057】

再び図9を参照して、ユーザ端末3において、コンテンツ配信装置1から送信される暗号化コンテンツは、コンテンツ蓄積部33に蓄積され、利用権利は、利用権利管理部34に入力される。利用権利管理部34は、取得した利用権利に含まれる復号鍵を用いて該当コンテンツに施された暗号を解読し、利用条件に従って暗号解読したコンテンツの再生処理等を、出力部37を通して実行する（ステップS96）。なお、取得された利用権利は、利用権利データベース35に格納され、コンテンツの再生回数や累積時間等の管理に利用される。

【0058】

上記処理によって、要求される利用条件に応じたコンテンツを配信することができる。

【0059】

（3）秘匿通信・通信切断処理

まず、図10を参照して、上述したコンテンツ利用処理において、利用権利の要求（図9のステップS91）、および、利用権利の配信（図9のステップS95）が複数回行われる際に、セキュリティ管理／通信部17、36で行われる、認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理の概略を説明する。

【0060】

ユーザ端末3とコンテンツ配信装置1との通信は、すべてユーザ端末3から開始されるリクエストメッセージと、前記リクエストメッセージに呼応してコンテンツ配信装置1から返信されるレスポンスメッセージからなる。リクエストとレスポンスとの対をフェーズと呼び、秘匿通信・通信切断処理は図10に示すとおり5種類のフェーズからなる。

【0061】

初期フェーズは、ユーザ端末3とコンテンツ配信装置1との間でセッションが確立された後、最初に1度だけ行われるフェーズである。

初回コマンド通信フェーズは、初期フェーズに続いて1度だけ行われるフェーズである。初回コマンド通信フェーズによって、最初のトランザクションが処理される。

【0062】

コマンド通信フェーズは、同一セッション内で2つ以上のトランザクションを処理する場合に発生するフェーズである。つまり、利用権利の要求および利用権利の配信が複数回行われる場合に、コマンド通信フェーズが用いられる。利用権利の要求および利用権利の配信が1度だけの場合は、コマンド通信フェーズは行われない。コマンド通信フェーズは、最初のトランザクションに続くトランザクション数だけ繰り返される。

【0063】

コミットフェーズは、すべてのトランザクション処理が終了した後に発生するフェーズである。

次に、図11～図15を参照して、上述したコンテンツ利用処理において、利用権利の要求（図9のステップS91）、および、利用権利の配信（図9のステップS95）が複数回行われる際の、各フェーズでの処理を説明する。

【0064】

図11は、コンテンツ利用処理におけるユーザ端末3とコンテンツ配信装置1との初期フェーズで行われる処理について記述している。図12は、初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末3において行われる処理について記述している。図13は初回コマンド通信フェーズで行われる処理について記述している。図14はコマンド通信フェーズで行われる処理について記述している。さらに、図15はコミットフェーズで行われる処理について記述している。

【0065】

まず、図11を参照して、ユーザ端末3とコンテンツ配信装置1との初期フェーズで行われる処理について説明する。ユーザ端末3のセキュリティ管理／通信部36に含まれる制御部304は、ユーザ指示処理部31からコンテンツ利用要求の送信を指示された場合、乱数発生部302で生成した乱数Rcと、固有情報

記憶部301に記憶している端末公開鍵証明書を、通信部305を介して、コンテンツ配信装置1へ送信する（ステップS1101）。

【0066】

コンテンツ配信装置1のセキュリティ管理／通信部17に含まれる制御部204は、通信部205を介してユーザ端末3から、乱数 R_c 、端末公開鍵証明書を受信すると、まず、固有情報記憶部201に記憶している認証局公開鍵証明書と、前記端末公開鍵証明書とを、暗号処理部203に与えることにより、前記端末公開鍵証明書の署名検証を行う（ステップS1102）。

【0067】

上記ステップS1102における署名検証の結果、検証失敗となった場合（ステップS1103, No）、制御部204は、要求を拒絶する旨を、通信部205を介してユーザ端末3へ通知する（ステップS1104）。

【0068】

一方、上記ステップS1102における署名検証の結果、検証が成功した場合（ステップS1103, Yes）、制御部204は、乱数発生部202で乱数 R_s 、 R_{s2} を生成し、暗号処理部203で、乱数 R_{s2} を入力としてDiffie-Hellmanパラメータ DH_s の生成を行う（ステップS1105）。

【0069】

さらに、制御部204は、通信ログデータベース206を検索し、トランザクション識別ビットが保存されているかを調べる。その結果、トランザクション識別ビットが保存されていない場合は、トランザクション識別ビット T を0とし、そうでない場合は、トランザクション識別ビット T を保存されているトランザクション識別ビットの値に設定する。その後、ユーザ端末3から受信した乱数 R_c 、トランザクション識別ビット T 、ステップS1105で生成した DH_s を連結したデータ（式1）の署名（式2）を暗号処理部203で生成する（ステップS1106）。ここで、トランザクション識別ビット T は、この初期フェーズに続く初期コマンド通信フェーズで処理されるコンテンツ要求トランザクションに対応付けられたビットであり、今後、通信切断が発生した場合には、このトランザクション識別ビット T を用いて、中断されたトランザクションの再開が行われる

【0070】

$$R_c || T || DH_s \quad (式1)$$

$$S(s, R_c || T || DH_s) \quad (式2)$$

制御部204は、ステップS1105で生成した乱数 R_s およびDiffie-Hellmanパラメータ DH_s と、トランザクション識別ビット T と、固有鍵情報記憶部201に記憶しているサーバ公開鍵証明書と、ステップS1106で生成した署名(式2)をユーザ端末3に通信部205を介して送信する(ステップS1107)。

【0071】

次に、図12を参照して、初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末3において行われる処理について説明する。

ユーザ端末3のセキュリティ管理/通信部36に含まれる制御部304は、通信部305を介してコンテンツ配信装置1から、乱数 R_s 、トランザクション識別ビット T 、Diffie-Hellmanパラメータ DH_s 、サーバ公開鍵証明書、および署名データを受信すると、まず、固有情報記憶部301に記憶している認証局公開鍵証明書と、前記サーバ公開鍵証明書とを、暗号処理部303に与えることにより、前記サーバ公開鍵証明書の署名検証を行う(ステップS1201)。

【0072】

上記ステップS1201における署名検証の結果、検証失敗となった場合(ステップS1202, No)、制御部304は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部31へ通知する(ステップS1203)。

【0073】

一方、上記ステップS1201における署名検証の結果、検証が成功した場合(ステップS1202, Yes)、制御部304は、ステップS1101で作成した乱数 R_c とステップS1107でコンテンツ配信装置1から受信したトランザクション識別ビット T 、および DH_s を結合したデータ(式3)を生成し、そのデータ(式3)、ステップS1107でコンテンツ配信装置1から受信した署

名データ（式2）、およびサーバ公開鍵証明書を暗号処理部303に入力し、署名データ（式2）の検証を行う（ステップS1204）。

【0074】

$$R_c || T || DH_s \quad (式3)$$

上記ステップS1204における署名検証の結果、検証失敗となった場合（ステップS1205, No）、制御部304は、コンテンツ利用要求を拒絶する旨を、ユーザ指示処理部31へ通知する（ステップS1203）。

【0075】

一方、上記ステップS1204における署名検証の結果、検証が成功した場合（ステップS1205, Yes）、ユーザ端末3は通信相手が確かにコンテンツ配信装置1であることが分かる（通信相手の認証）。制御部304は、乱数発生部302で乱数Rc2を生成し、生成した乱数Rc2を暗号処理部303の入力としてDiffie-HellmanパラメータDHcを生成する（ステップS1206）。

【0076】

さらに、制御部304は、ステップS1107でコンテンツ配信装置1から受信したDHsと、ステップS1206で生成したRc2とから、暗号処理部303でセッション鍵KSを生成する（ステップS1207）。

【0077】

その後、制御部304は、ステップS1107でコンテンツ配信装置1から受信したトランザクション識別ビットTを通信ログデータベース306に記憶する（ステップS1208）。これにより、トランザクション通信ビットTに対応するコンテンツ利用権利要求トランザクションが開始され、レスポンス待ち状態であることがデータベースに保存される。これ以降、通信切断などによりトランザクションが中断された場合には、トランザクションTの処理を再開すればよいこととなる。

【0078】

制御部304は、ステップS1107でコンテンツ配信装置1から受信した乱数RsとステップS1206で生成したDHcを連結したデータ（式4）の署名

(式5) を暗号処理部303で生成し、ステップS1207で生成したセッション鍵KSで、ステップS1107で受信したトランザクション識別ビットTとコンテンツ利用要求メッセージMを暗号化する(ステップS1209)。コンテンツ利用要求メッセージは、少なくとも利用するコンテンツのコンテンツ識別子を含む。暗号化データにはシーケンス番号Seqとハッシュ値hを付加する(式6)。ハッシュの対象データはシーケンス番号Seqとコンテンツ利用要求メッセージMとする。シーケンス番号は、セッションが開始されたとき、つまり、初期フェーズが開始される際に0にリセットされ、メッセージの送信および受信の度に1ずつ加算される通し番号である。

【0079】

$$Rs || DHc \quad (式4)$$

$$S(c, Rs || DHc) \quad (式5)$$

$$E(KS, Seq || T || M || h) \quad (式6)$$

制御部304は、ステップS1206で生成したDHcと、ステップS1209で生成した署名(式5)と暗号化データ(式6)をコンテンツ配信装置1に通信部305を介して送信する(ステップS1210)。

【0080】

次に、図13を参照して、初回コマンド通信フェーズで行われる処理について説明する。

コンテンツ配信装置1のセキュリティ管理/通信部17に含まれる制御部204は、通信部205を介してユーザ端末3から、Diffie-HellmanパラメータDHc、署名データ、および暗号化データを受信すると、ステップS1105で作成した乱数RsとステップS1210でユーザ端末3から受信したDHcを結合したデータ(式7)を生成し、その生成データ(式7)、ステップS1210でユーザ端末3から受信した署名データ、および端末公開鍵証明書を暗号処理部203に入力し、署名データの検証を行う(ステップS1301)。

【0081】

$$Rs || DHc \quad (式7)$$

上記ステップS1301における署名検証の結果、検証失敗となった場合(ス

テップS1302, No)、制御部204は、コンテンツ利用要求を拒絶する旨を、通信部205を介してユーザ端末3へ通知する(ステップS1303)。

【0082】

一方、上記ステップS1301における署名検証の結果、検証が成功した場合(ステップS1302, Yes)、コンテンツ配信装置1は通信相手が確かにユーザ端末3であることが分かる(通信相手の認証)。制御部204は、ステップS1210でユーザ端末3から受信したDHcと、ステップS1105で生成したRs2とから、暗号処理部203でセッション鍵KSを生成する。その後、ステップS1210で受信した暗号化データと生成したKSを暗号処理部203に入力し暗号化データの復号を行い、シーケンス番号とハッシュ値のチェックを行う(ステップS1304)。

【0083】

さらに、制御部204は、通信ログデータベースを検索し、トランザクション識別ビットを取得する。その結果、トランザクション識別ビットが存在しない、もしくは、その値がステップS1210で受信したトランザクション識別ビットTと一致しない場合(ステップS1305, No)、コンテンツ配信装置1は、要求トランザクションを新規のものと判断し、制御部204は、ステップS1301でユーザ端末3から受信したトランザクション識別ビットTを通信ログデータベース206に記憶する(ステップS1306)。これにより、トランザクション識別ビットTに対応するコンテンツ利用権利要求トランザクションが、このステップまで完了したことがデータベースに保存される。よって、これ以降、通信切断などによりトランザクションが中断された場合には、トランザクションTの処理を再開すればよいこととなる。

【0084】

その後、制御部204はユーザ権利生成部14に新規トランザクションとして、ステップS1210でユーザ端末3から受信したコンテンツ利用要求を通知する(ステップS1307)。

【0085】

一方、トランザクション識別ビットが既に存在し、その値がステップS121

0で受信したトランザクション識別ビットTと一致した場合（ステップS1305, Yes）、制御部204は、ユーザ権利生成部14に再開トランザクションとして、ステップS1210でユーザ端末3から受信したコンテンツ利用要求を通知する（ステップS1308）。

【0086】

制御部204は、シーケンス番号とユーザ権利作成部14で作成された利用権利とそれらのハッシュ値をステップS1304で生成したセッション鍵KSを用いて暗号処理部203で暗号化して、通信部205を介してユーザ端末3に送信する（ステップS1309）。ここで、送信される利用権利は、コンテンツ配信装置1とユーザ端末3のみで生成可能なセッション鍵KSで暗号化されているため、第三者が盗聴することはできない。

【0087】

ユーザ端末3のセキュリティ管理／通信部36に含まれる制御部304は、通信部305を介してコンテンツ配信装置1から、暗号化データを受信すると、まず、暗号処理部303でセッション鍵KSを用いて暗号化データの復号を行い、シーケンス番号、利用権利、ハッシュ値を復元する。その後、シーケンス番号とハッシュ値のチェックを行い、利用条件をユーザ指示処理部31へ通知する。さらに、通信ログデータベース306に保存しているトランザクション識別ビットを反転させる。（ステップS1310）。これにより、トランザクション識別ビットTに対応するトランザクションが完了したこととなる。

【0088】

この後、引き続きトランザクションがある場合にはステップS1401へ、そうでない場合はステップS1501へ移る。

次に、図14を参照して、コマンド通信フェーズで行われる処理について説明する。

【0089】

制御部304は、初期化フェーズで生成したセッション鍵KSで、通信ログデータベース306に記憶するトランザクション識別ビットTとコンテンツ利用要求メッセージMを暗号化する（ステップS1401）。コンテンツ利用要求メッ

セージは、少なくとも利用するコンテンツのコンテンツ識別子を含む。暗号化データにはシーケンス番号Seqとハッシュ値hを付加する。ハッシュの対象データはシーケンス番号Seqとコンテンツ利用要求メッセージMとする。

【0090】

制御部304は、ステップS1401で生成した暗号化データをコンテンツ配信装置1に通信部305を介して送信する（ステップS1402）。

コンテンツ配信装置1のセキュリティ管理／通信部17に含まれる制御部204は、通信部205を介してユーザ端末3から暗号化データを受信すると、暗号化データと初回コマンド通信フェーズで生成した生成したKSを暗号処理部203に入力し暗号化データの復号を行い、シーケンス番号とハッシュ値のチェックを行う（ステップS1403）。

【0091】

さらに、制御部204は、通信ログデータベースを検索し、ステップS1402でユーザ端末3から受信したトランザクション識別ビットTと通信ログデータベースに保持するトランザクション識別ビットと一致するかを調べる。その結果、一致しない場合（ステップS1404, No）、制御部204は、ステップS1402でユーザ端末3から受信したTに通信ログデータベース206の内容を変更する（ステップS1405）。これにより、トランザクション識別ビットTに対応する新規コンテンツ利用権利要求トランザクションが、このステップまで完了したことがデータベースに保存される。よって、これ以降、通信切断などによりトランザクションが中断された場合には、トランザクションTの処理を再開すればよいこととなる。

【0092】

その後、制御部204はユーザ権利生成部14に新規トランザクションとして、ステップS1402でユーザ端末3から受信したコンテンツ利用要求を通知する（ステップS1406）。

【0093】

一方、トランザクション識別ビットTが通信ログデータベース206に保持するトランザクション識別ビットと一致する場合（ステップS1404, Yes）

、制御部 204 は、ユーザ権利生成部 14 に再開トランザクションとして、ステップ S1402 でユーザ端末 3 から受信したコンテンツ利用要求を通知する（ステップ S1407）。

【0094】

制御部 204 は、シーケンス番号とユーザ権利作成部 14 で作成された利用権利とそれらのハッシュ値を初回コマンド通信フェーズで生成したセッション鍵 KS を用いて暗号処理部 203 で暗号化して、通信部 205 を介してユーザ端末 3 に送信する（ステップ S1408）。ここで、送信される利用権利は、コンテンツ配信装置 1 とユーザ端末 3 のみで生成可能なセッション鍵 KS で暗号化されているため、第三者が盗聴することはできない。

【0095】

ユーザ端末 3 のセキュリティ管理／通信部 36 に含まれる制御部 304 は、通信部 305 を介してコンテンツ配信装置 1 から、暗号化データを受信すると、まず、暗号処理部 303 でセッション鍵 KS を用いて暗号化データの復号を行い、シーケンス番号、利用権利、ハッシュ値を復元する。その後、シーケンス番号とハッシュ値のチェックを行い、利用条件をユーザ指示処理部 31 へ通知する。さらに、通信ログデータベース 306 に保存しているトランザクション識別ビット T を反転する。（ステップ S1409）。これにより、トランザクション識別ビット T に対応するトランザクションが完了したこととなる。

【0096】

この後、引き続きトランザクションがある場合にはステップ S1401 へ、そうでない場合はステップ S1501 へ移る。

最後に、図 15 を参照して、コミットフェーズで行われる処理を説明する。

【0097】

制御部 304 は、初期化フェーズで生成したセッション鍵 KS で、コミットメッセージを暗号化する（ステップ S1501）。

制御部 304 は、ステップ S1501 で生成した暗号化データをコンテンツ配信装置 1 に通信部 305 を介して送信する（ステップ S1502）。

【0098】

コンテンツ配信装置 1 のセキュリティ管理／通信部 17 に含まれる制御部 204 は、通信部 205 を介してユーザ端末 3 から暗号化データを受信すると、暗号化データと初回コマンド通信フェーズで生成した生成した K S を暗号処理部 203 に入力し暗号化データの復号を行う（ステップ S 1503）。

【0099】

さらに、制御部 204 は、通信ログデータベース 206 に記憶しているトランザクション識別ビットを削除する（ステップ S 1504）。

制御部 204 は、ACK メッセージを初回コマンド通信フェーズで生成したセッション鍵 K S を用いて暗号処理部 203 で暗号化して、通信部 205 を介してユーザ端末 3 に送信する（ステップ S 1505）。

【0100】

ユーザ端末 3 のセキュリティ管理／通信部 36 に含まれる制御部 304 は、通信部 305 を介してコンテンツ配信装置 1 から、暗号化データを受信すると、まず、暗号処理部 303 でセッション鍵 K S を用いて暗号化データの復号を行い、ACK メッセージを復元し、コミット処理が完了したことをユーザ指示処理部 31 へ通知する。その後、通信ログデータベース 306 に保存しているトランザクション識別ビット T を削除する。（ステップ S 1506）。

【0101】

なお、通信切断後のトランザクション再開処理は、ユーザ指示処理部 31 からのトランザクション再開処理要求によって開始され、初期フェーズを処理した後、通信切断により中断されているトランザクションに対応するトランザクション識別ビット（通信ログデータベースに保存されているトランザクション識別ビット）T を用いて、初回コマンド通信フェーズによって再開される。この初回コマンド通信フェーズで送信されるコンテンツ利用要求メッセージは、ユーザ指示処理部 31 が再度、制御部 304 に渡してもよいし、制御部 304 が通信ログデータベースにトランザクション識別ビットを保存する際にコンテンツ利用要求メッセージも保存するようにし、その保存しておいたメッセージを利用してもよい。

【0102】

上記処理により、ユーザ端末 3 の認証処理、利用権利の盗聴・改ざん防止処理

、および通信切断対策処理を行うことが可能となる。

本実施の形態で示した通信プロトコルにおいて、 n 個のトランザクションを処理する際の通信往復回数は、初期フェーズで1往復、初回コマンド通信フェーズで1往復、コマンド通信フェーズで $n-1$ 往復、コミットフェーズで1往復となり、合計 $n+2$ 回となる。

【0103】

なお、本実施の形態で用いた暗号アルゴリズム、セッション鍵共有アルゴリズム、証明書フォーマットなどは、同等の機能を持つものであれば、必ずしも記載したものを用いる必要はない。例えば、データの暗号アルゴリズムにはTriple DESを用いてもよい。また、暗号化データに付与されるハッシュ値は、CRCなどのチェックサム値を用いてもよい。さらに、SACプロトコルには公開鍵暗号方式の代わりに共通鍵暗号方式を用いてもよい。

【0104】

なお、本実施の形態では、ユーザ端末3からの端末公開鍵証明書は、初期化フェーズ（図11のステップS1101）において送信したが、初回コマンド通信フェーズ（図12のステップS1210）において送信してもよい。これにより、コンテンツ配信装置1は、装置内に上記データを保持しておく必要がなくなる。この場合、コンテンツ配信装置1での端末公開鍵証明書の署名検証処理（図11のステップS1102）は、初回コマンド通信フェーズの最初（図13のステップS1301の直前）で行うこととなる。

【0105】

なお、ステップS1107において、コンテンツ配信装置1からユーザ端末3へ送信されるデータに、ユーザ端末3から受信した乱数 R_c を含めてもよい。つまり、コンテンツ配信装置1から送信されるデータは、乱数 R_c 、乱数 R_s 、トランザクション識別ビット T 、パラメータ DH_s 、署名データとなる。これにより、ユーザ端末3は、乱数 R_c を端末内に保持しておく必要がなくなる。同様に、ステップS1210において、ユーザ端末3からコンテンツ配信装置1へ送信されるデータに、コンテンツ配信装置1から受信した乱数 R_s を含めてもよい。つまり、コンテンツ配信装置1から送信されるデータは、乱数 R_s 、パラメータ

DHc、署名データ、暗号化データとなる。

【0106】

なお、本実施の形態においては、ユーザ端末3がコンテンツ配信装置1を認証する処理も含まれているが、特に必要がない場合には、認証処理を除いてもよい。

【0107】

なお、本実施の形態においては、コマンド通信フェーズでトランザクション識別ビットの一致判定を行っているが、特に必要が無い場合には、判定処理を除いてもよい。この場合、コマンド通信フェーズで処理されるトランザクションは常に新規トランザクションとして処理される。

【0108】

なお、本実施の形態においては、トランザクション識別ビットをコンテンツ配信装置1から送信するようにしているが、これを省略してもよい。つまり、初期フェーズにおけるコンテンツ配信装置1の処理および、初期フェーズにおけるメッセージ中のトランザクション識別ビットに関する情報は省略される。

【0109】

なお、本実施の形態においては、ステップS1308およびステップS1407においてユーザ権利の作成を行う際に、セキュリティ管理／通信部17から再開トランザクションとして指示された場合には、登録内容の更新を行わないとしたが、再度、コンテンツ利用要求を評価し、ユーザ権利の作成をやり直してもよい。これにより、新規トランザクションの発行と再開トランザクションの発行の間に起こった状況変化に対応することが可能となる。例を挙げれば、新規トランザクション発行時には、コンテンツの利用有効期限内であったので利用権利の作成・送信を行ったが、再開トランザクションとして再度要求が行われたときには、コンテンツの利用有効期限を越えたいた場合が考えられる。この場合には、再開トランザクションに対しては利用権利の作成・発行は行わない。

【0110】

また、本実施の形態においては、通信切断によって処理途中のトランザクションのキャンセル処理を含めてもよい。キャンセル処理を行う場合、通信切断後の

初回コマンド通信フェーズで、レスポンスをまだ受信していないトランザクションに対応するトランザクション識別ビットT（通信ログデータベース306に保存しているもの）を含むキャンセルメッセージをユーザ指示処理部31の指示によりユーザ端末3から送信する。キャンセルメッセージを受信したコンテンツ配信装置1は、ユーザ権利作成部14にその旨を通知し、処理途中のトランザクションを処理前の状態にロールバックさせる。その後、コンテンツ配信装置1はユーザ端末3に対して、ACKメッセージを送信する。

【0111】

また、コンテンツ配信装置1とユーザ端末3との間の2つのコンテンツ利用要求処理を処理Aおよび処理Bとすると、処理Aの終了後に、一旦、通信切断を行わなければいけない場合、通常は、処理Bの開始時には再度認証処理を行い、新たなセッション鍵を作成し直すが、処理Bの応答時間を削減したい場合には、処理Bでの認証処理を除くために、処理Aでのセッション鍵をコンテンツ配信装置1とユーザ端末3の双方で記憶しておき、再利用してもよい。

【0112】

なお、本実施の形態においては、コンテンツ配信装置1はセッション鍵の利用制限を設けてもよい。例えば、セッション鍵の再利用回数が規定の上限を超えた場合、セッション鍵が最初に作成されたから規定の時間が経過した場合、セッション鍵が最初に作成されてから規定の通信データ量を超えた場合、予め決められたコンテンツあるいは利用権利を配信する場合、あるいは、予め決められたユーザ端末3に配信する場合などに、コンテンツ配信装置1はユーザ端末3にセッション鍵再利用不可通知を行う。セッション鍵再利用不可通知を受信したユーザ端末3は、セッション鍵を生成しなおす。つまり、初期フェーズから通信をやり直す。

【0113】

なお、本実施の形態においては、コンテンツ配信装置1とユーザ端末3との間のプロトコルとして説明を行ったが、ユーザ端末同士でのライセンス交換にも適用可能である。例えば、家庭内のユーザ端末同士でライセンスを移動させる場合に適用できる。その際、同一家庭内のユーザ端末であるというグループ識別子が

予め、あるいは、購入後の設定により指定されているものとする。ユーザ端末間でライセンスを移動させる際に本実施の形態で示したプロトコルを適用する場合、ライセンスの移動元端末をコンテンツ配信装置 1 に、ライセンスの移動先端末をユーザ端末 3 と捉えればよい。なお、ライセンスの移動を同一家庭内、つまり、同一グループ識別子を持つもの同士に限る場合には、ライセンス配信先端末からライセンス配信元端末にグループ識別子を送信し、ライセンス配信元端末が同一グループ識別子かどうかを判定し、同一である場合のみライセンスの送信を行うようにする。グループ識別子の送信は、盗聴・改ざん・成りすましを防ぐ方法であれば、どのような方法であってもよい。例えば、初回コマンド通信フェーズの暗号化データに含めてもよい。また、グループ識別子そのものを送信せず、グループ識別子のハッシュ値を用いてもよい。さらに、別途、グループ識別子ハッシュ送信フェーズを初期フェーズの後に設けて、セッション鍵で暗号化したグループ識別子ハッシュを送信してもよい。

【0114】

なお、本実施の形態で示したコンテンツ配信システムの各構成要素は、ハードウェアで実現しても、ソフトウェアで実現してもよい。

【0115】

【発明の効果】

以上のように本発明によれば、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するとともに、複数トランザクション処理を行う場合においても、サーバ装置・端末装置間の通信往復回数を減少させ、さらに、上記機能を実現するためにサーバ装置と端末装置で管理・保持する情報が少ないプロトコルを実現するシステムおよび装置を提供する。これにより、ユーザが要求を出してから、応答を得るまでの待ち時間を短縮させることが可能なコンテンツ配信システムを提供することができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係るコンテンツ配信システムの構成を示すブロック図

【図 2】

本発明の一実施形態に係るコンテンツ配信装置のセキュリティ管理／通信部の詳細な構成を示すブロック図

【図 3】

本発明の一実施形態に係るユーザ端末のセキュリティ管理／通信部の詳細な構成を示すブロック図

【図 4】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ購入に関する処理を説明するフローチャート

【図 5】

コンテンツ権利データベース 19 に格納されているコンテンツに関する情報の一例を概念的に示す図

【図 6】

ユーザデータベース 18 に格納されているユーザ情報の一例を概念的に示す図

【図 7】

ユーザ所有権利データベース 20 に格納されているユーザが所有する権利の情報の一例を概念的に示す図

【図 8】

コンテンツデータベース 21 に格納されているコンテンツ情報の一例を概念的に示す図

【図 9】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用に関する処理を説明するフローチャート

【図 10】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 との認証処理、利用権利の盗聴・改ざん防止処理、および通信切断対策処理の概略を説明する図

【図 11】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末 3 とコンテンツ配信装置 1 との初期フェーズにて行わ

れる処理を説明するフローチャート

【図 12】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末3とコンテンツ配信装置1との初期フェーズ後、初回コマンド通信フェーズを開始する前にユーザ端末3において行われる処理を説明するフローチャート

【図 13】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末3とコンテンツ配信装置1との初回コマンド通信フェーズにて行われる処理を説明するフローチャート

【図 14】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末3とコンテンツ配信装置1とのコマンド通信フェーズにて行われる処理を説明するフローチャート

【図 15】

本発明の一実施形態に係るコンテンツ配信システムで行われるコンテンツ利用処理において、ユーザ端末3とコンテンツ配信装置1とのコミットフェーズにて行われる処理を説明するフローチャート

【符号の説明】

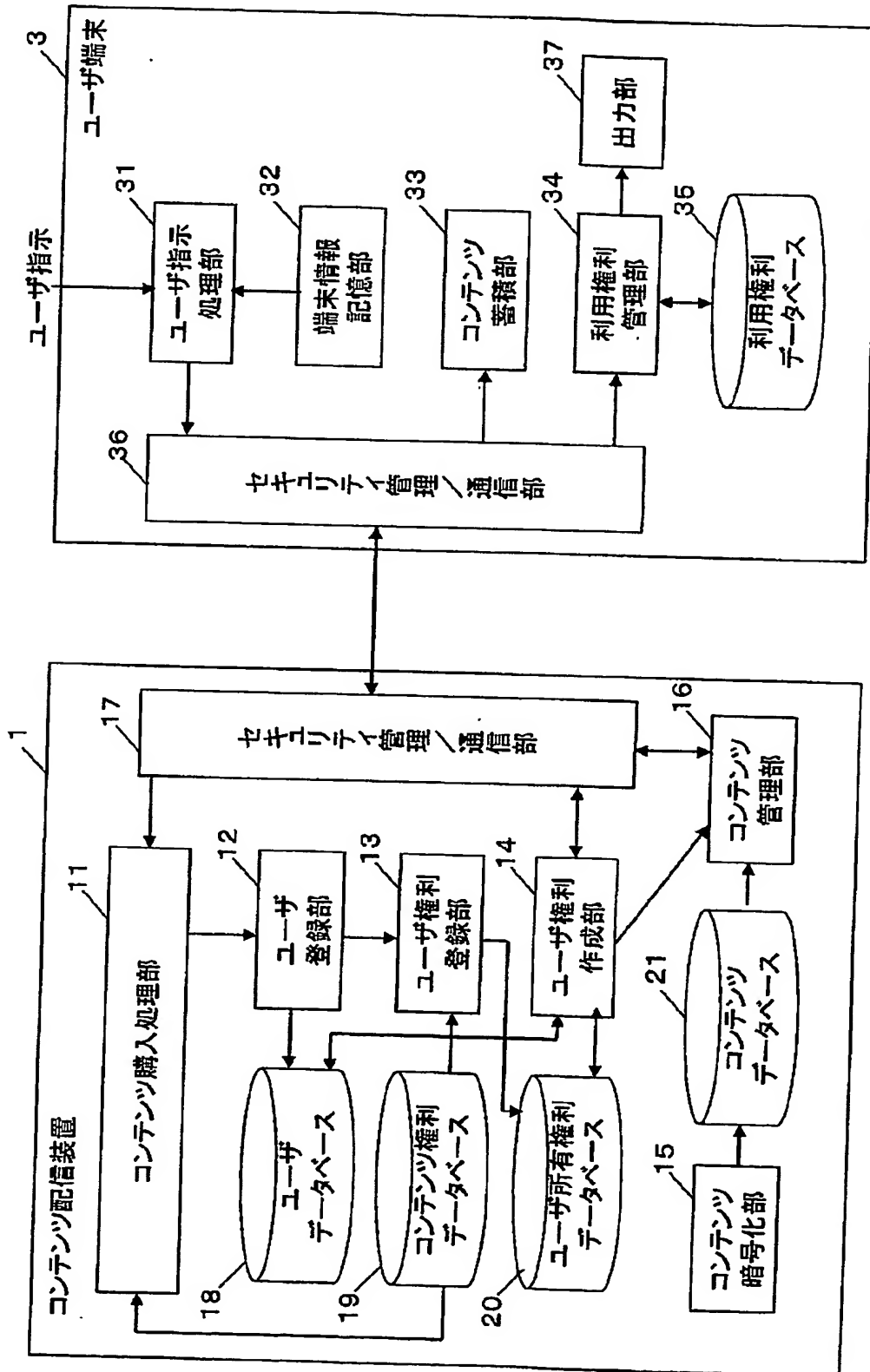
- 1 コンテンツ配信装置
- 3 ユーザ端末
 - 11 コンテンツ購入処理部
 - 12 ユーザ登録部
 - 13 ユーザ権利登録部
 - 14 ユーザ権利作成部
 - 15 コンテンツ暗号化部
 - 16 コンテンツ管理部
 - 17、36 セキュリティ管理／通信部
 - 18 ユーザデータベース

- 1 9 コンテンツ権利データベース
- 2 0 ユーザ所有権利データベース
- 2 1 コンテンツデータベース
- 3 1 ユーザ指示処理部
- 3 2 端末情報記憶部
- 3 3 コンテンツ蓄積部
- 3 4 利用権利管理部
- 3 5 利用権利データベース
- 3 7 出力部
- 2 0 1、3 0 1 固有鍵情報記憶部
- 2 0 2、3 0 2 乱数発生部
- 2 0 3、3 0 3 暗号処理部
- 2 0 4、3 0 4 制御部
- 2 0 5、3 0 5 通信部
- 2 0 6、3 0 6 通信ログデータベース

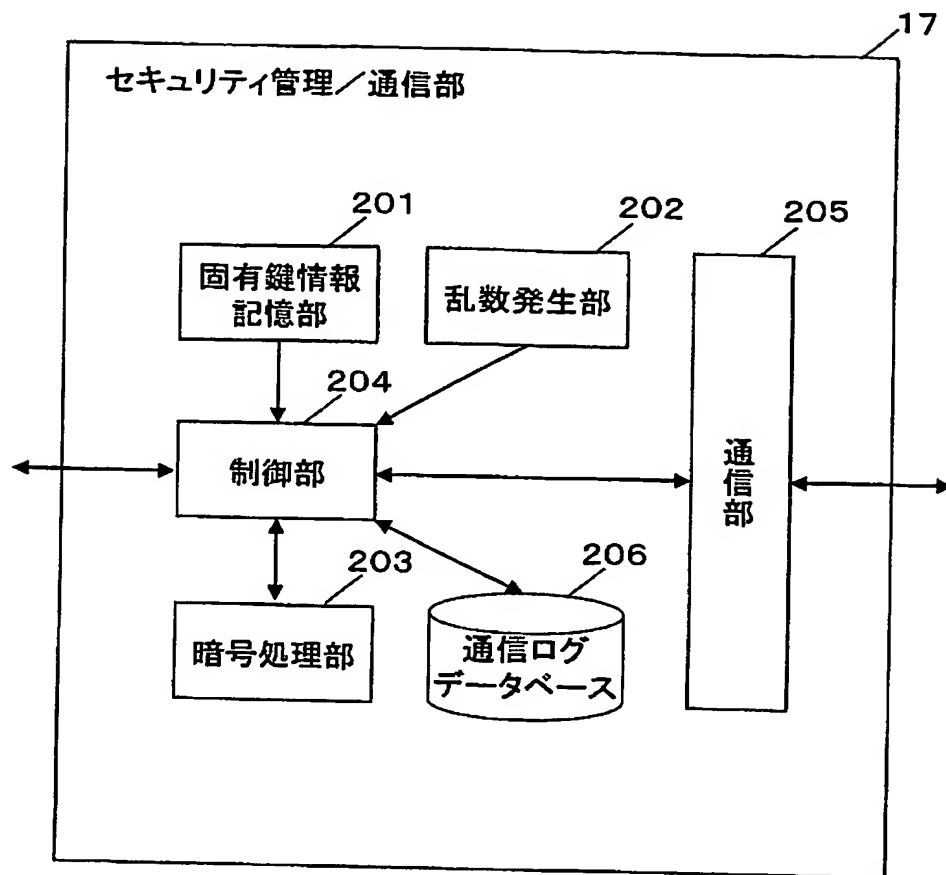
【書類名】

図面

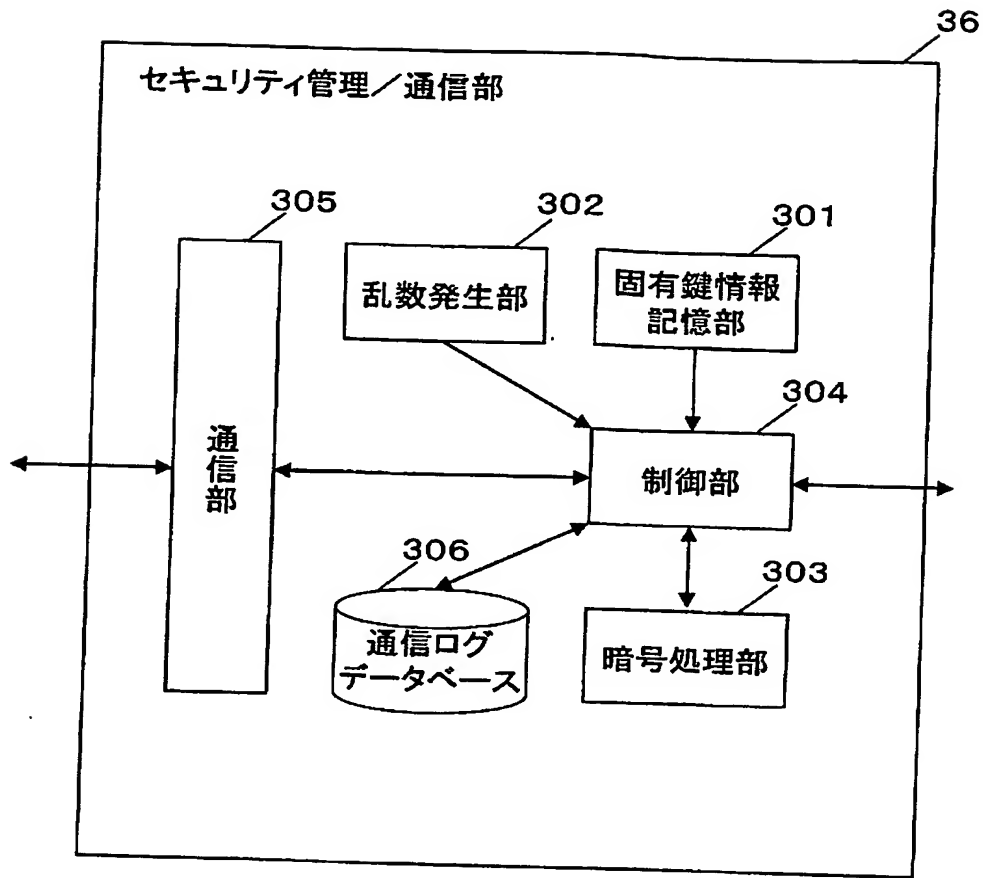
【図 1】



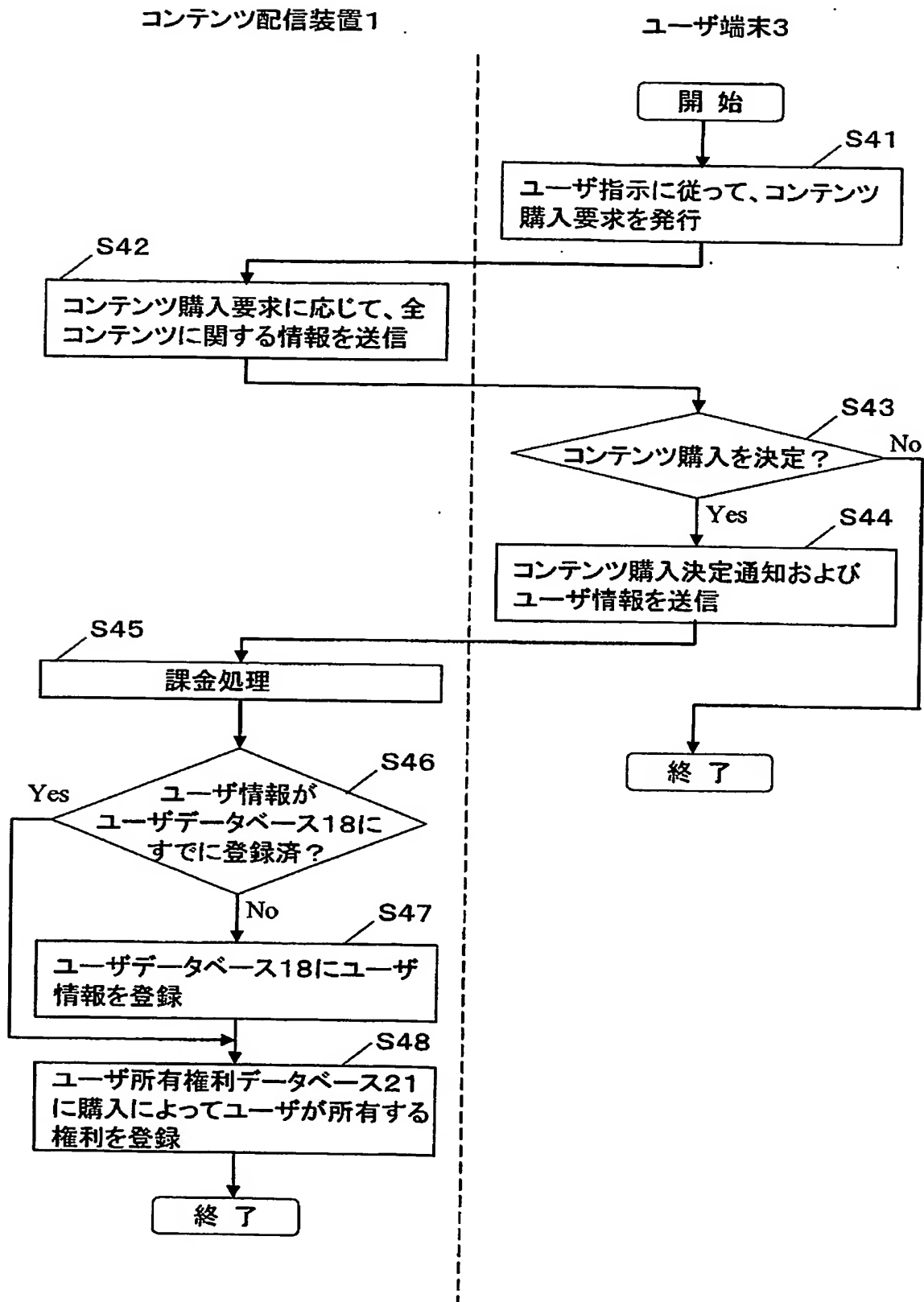
【図 2】



【図 3】



【図 4】



【図 5】

コンテンツ名	コンテンツID	利用条件	料金
映画A	112233	再生回数=2	400円
音楽B	334567	再生回数=5 累積再生時間=1H	500円 1000円
ゲームC	321098	累積再生時間=2H 無制限	700円 2000円

【図 6】

ユーザID	ユーザ名	端末ID	電話番号
0001	一朗	1234567	06-XXXX-XXXX
0002	太郎	1170930	03-YYYY-YYYY

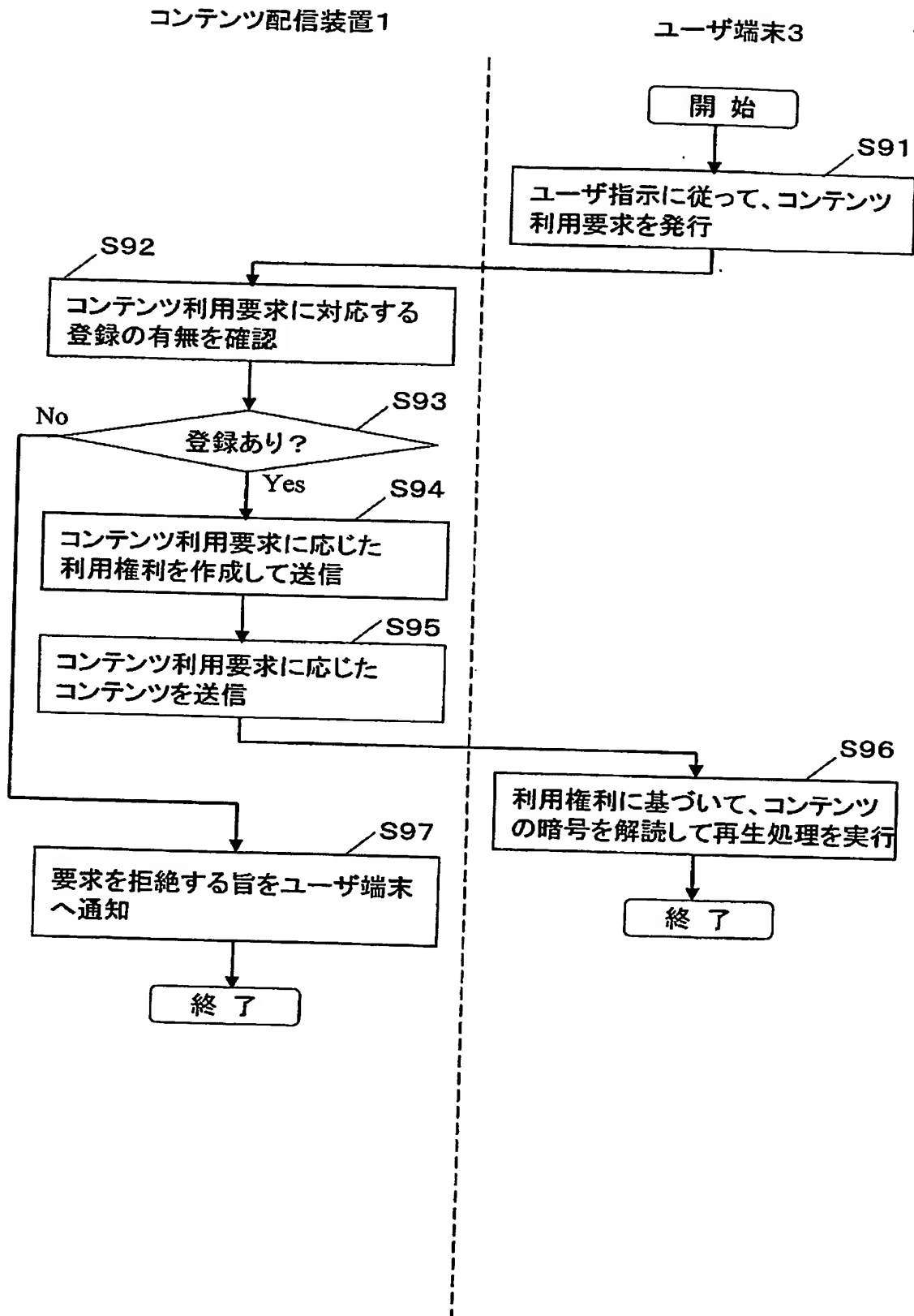
【図 7】

ユーザID	コンテンツID	利用条件
0001	112233	再生回数=2
0002	321098	累積再生時間=2H

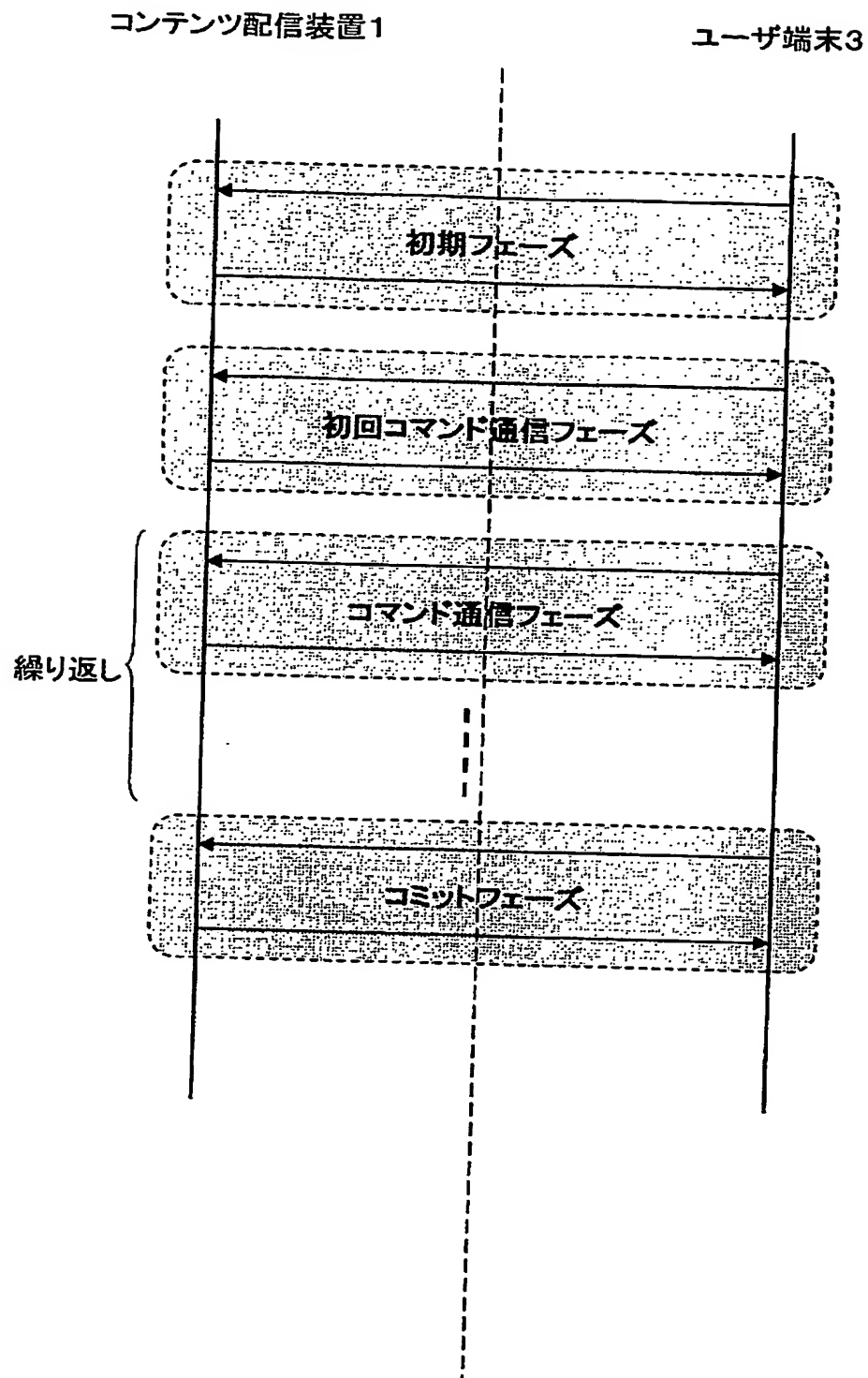
【図 8】

コンテンツID	コンテンツ名	コンテンツ暗号鍵	ファイル名
112233	映画A	0123456789..	movieA.mpg
234567	音楽B	7361278168..	musicB.wav

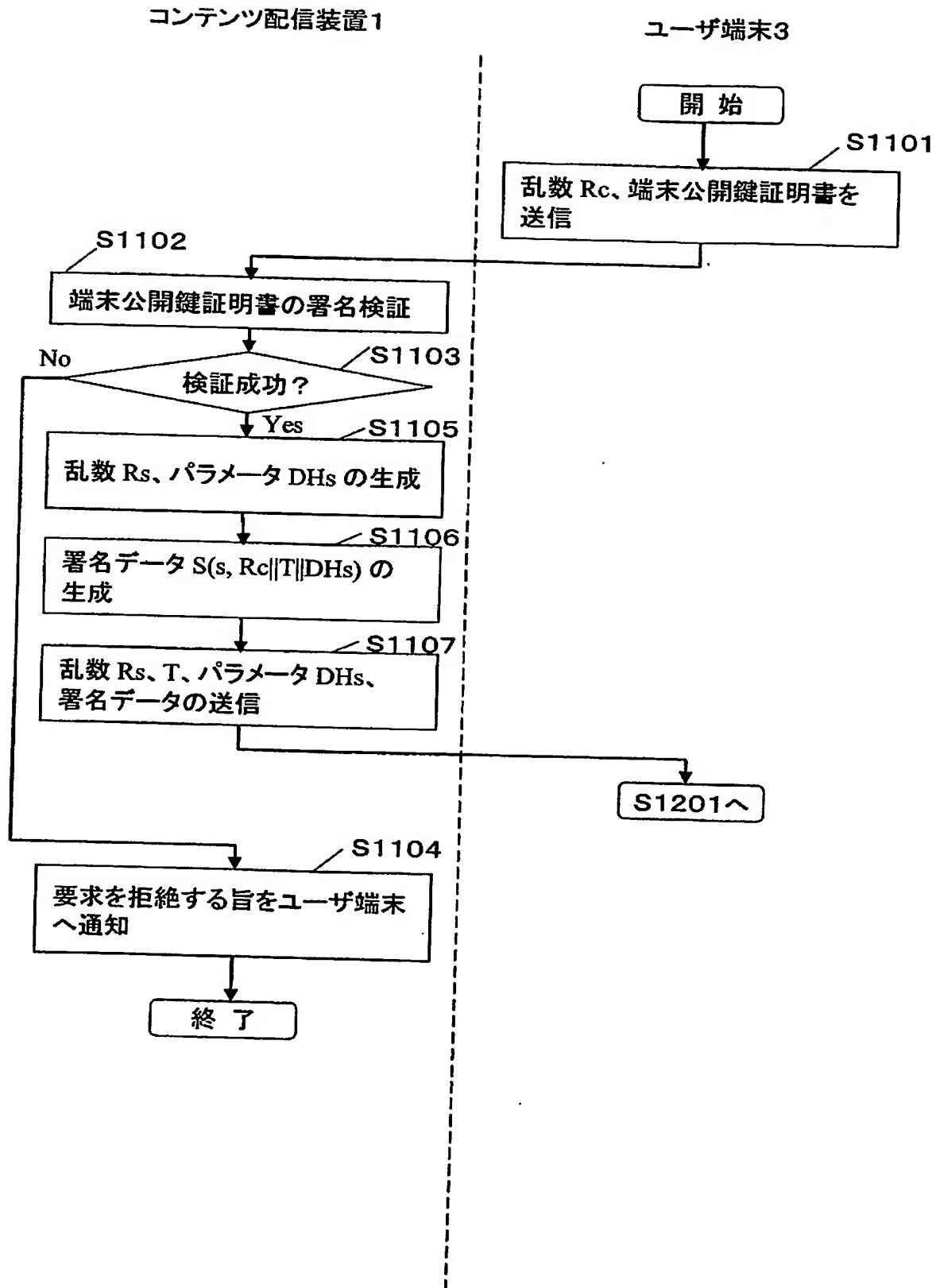
【図 9】



【図 10】



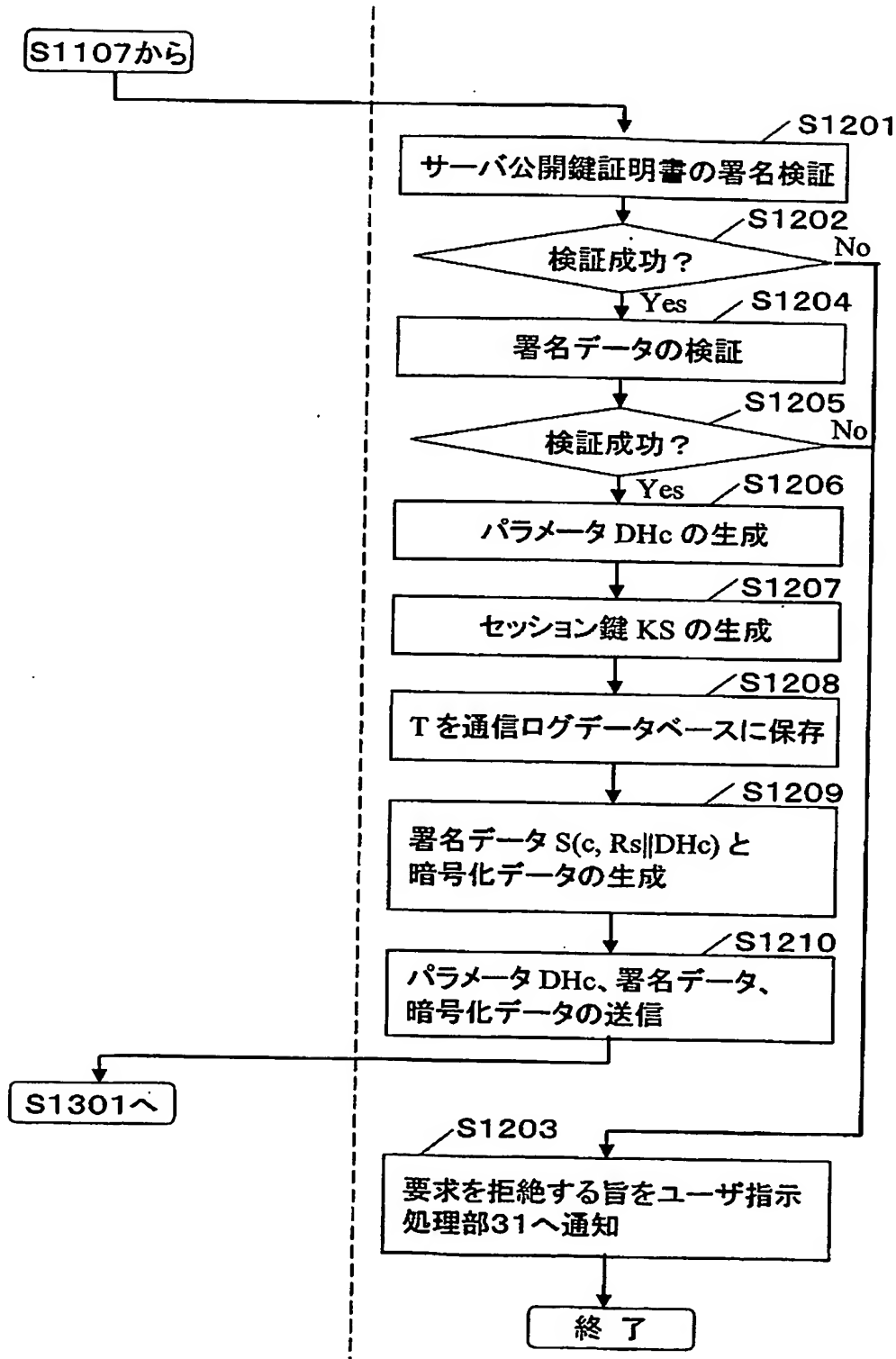
【図 11】



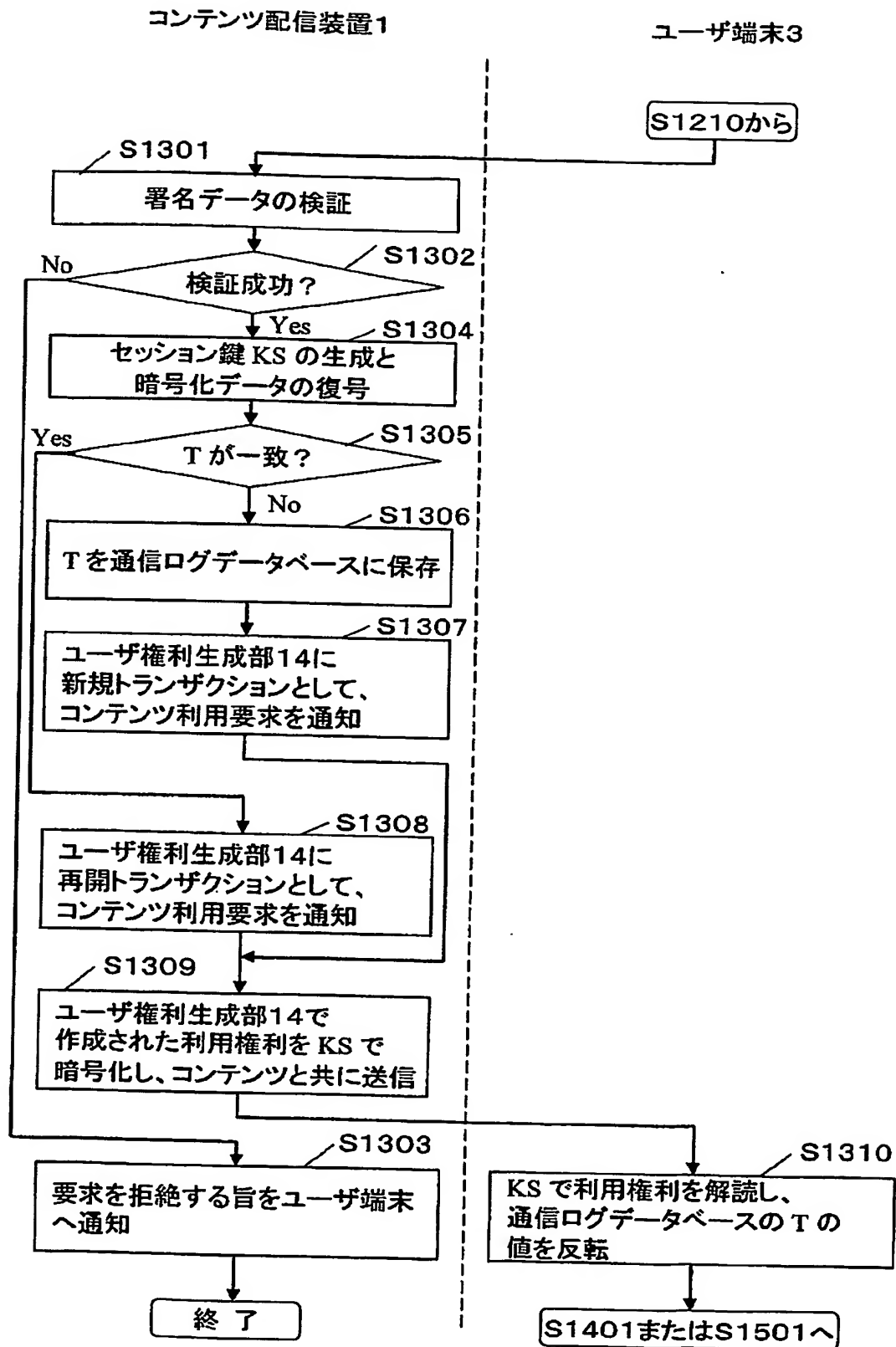
【図 12】

コンテンツ配信装置1

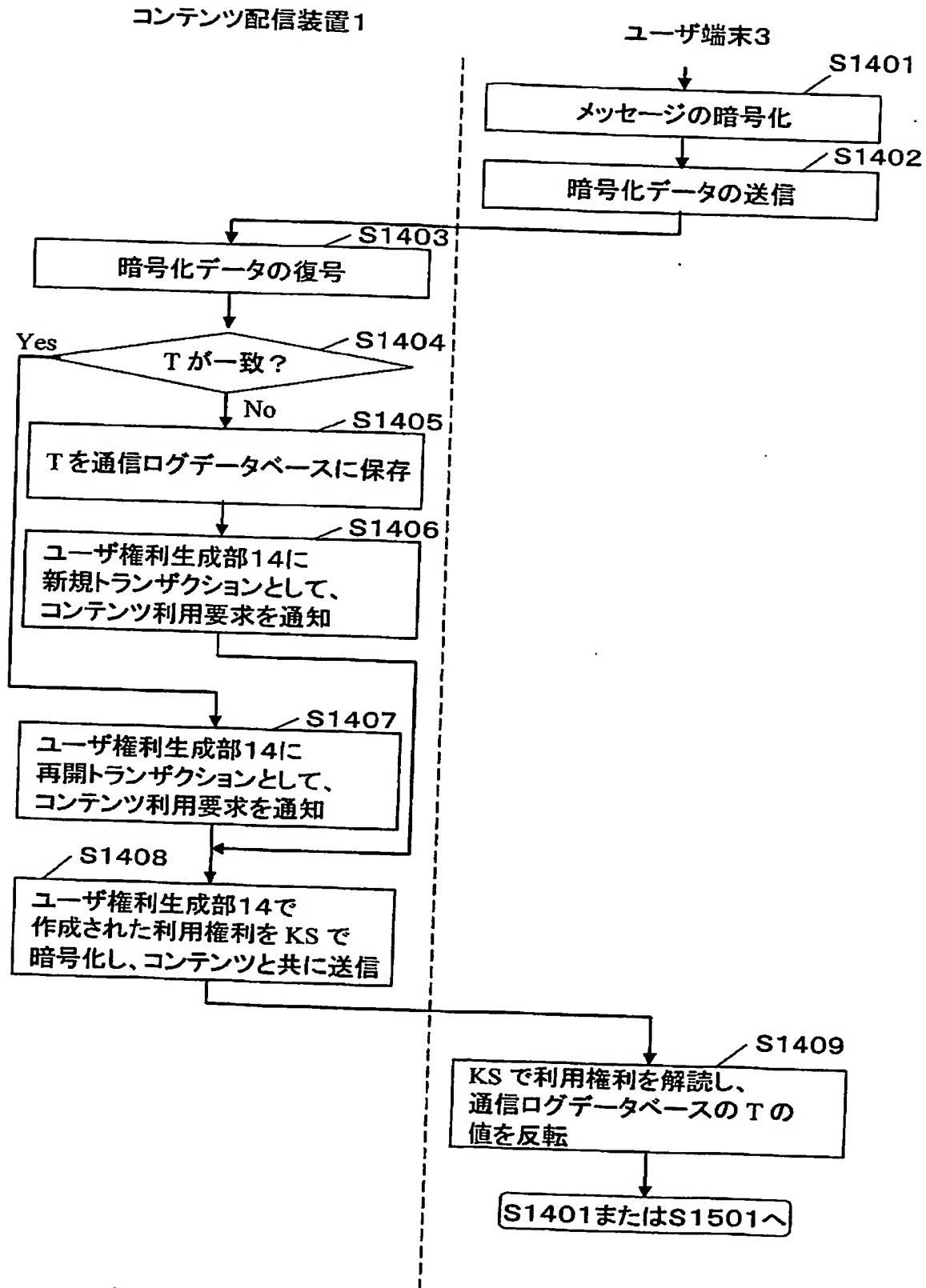
ユーザ端末3



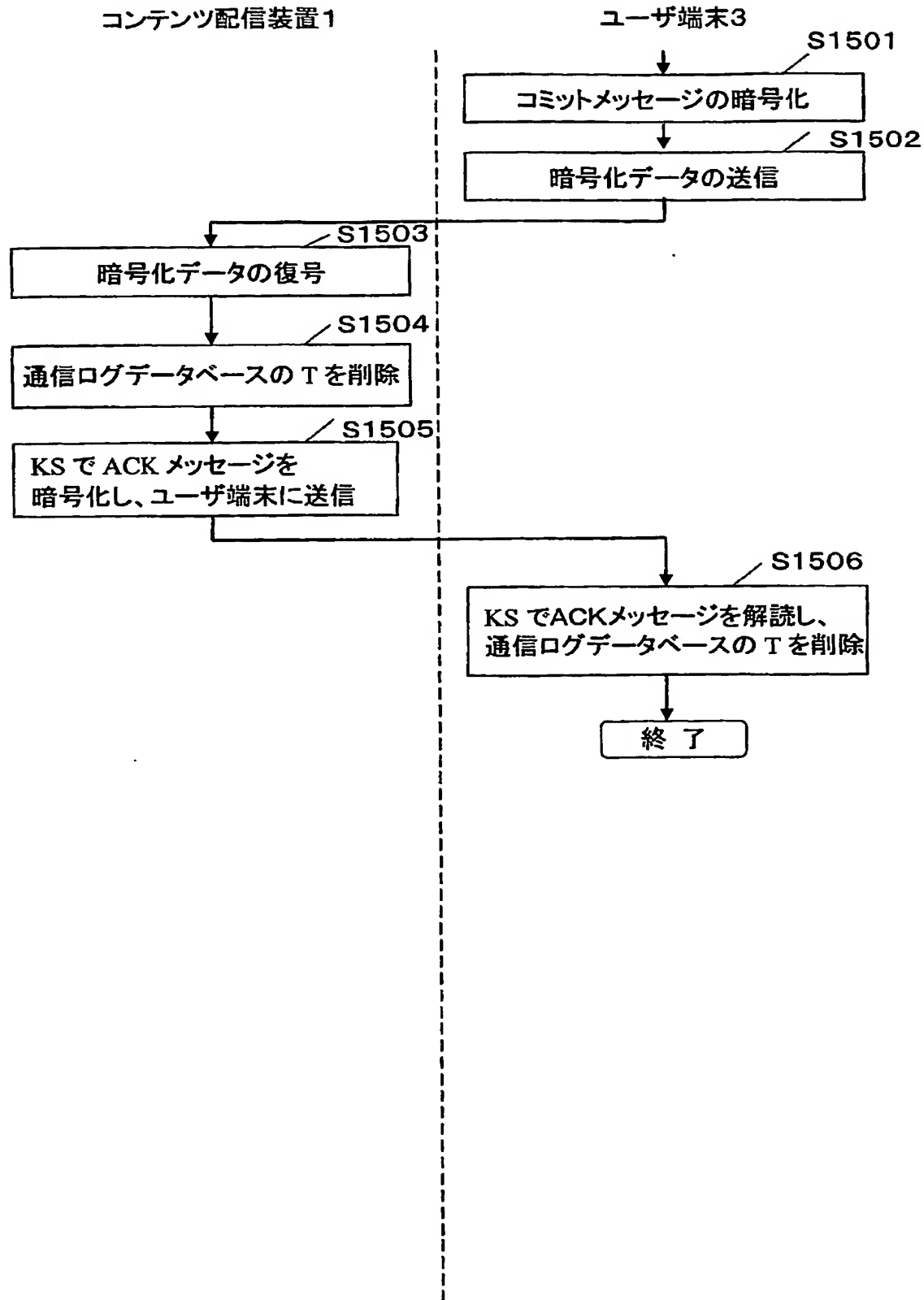
【図13】



【図 14】



【図 15】



【書類名】 要約書

【要約】

【課題】 SACプロトコルや通信切断対策プロトコルの双方を利用することで、ライセンスの盗聴・改ざんの防止、通信相手の認証、通信切断対策のすべての機能を実現するためには、双方のプロトコルで必要な通信往復回数が必要となるという課題があった。

【解決手段】 ユーザにコンテンツの利用に対するライセンスを提供するサーバ装置と、前記サーバ装置から取得した前記ライセンスに基づいて前記コンテンツの利用を制御する端末装置とから構成されるデジタルコンテンツ配信システムであって、前記サーバ装置および前記端末装置は、少なくともトランザクション識別ビットを記憶するトランザクション識別ビット記憶手段を持つにより、複数トランザクション処理を行う場合において、ユーザに対する応答時間を削減する。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2003-049710
受付番号	50300311722
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 2月27日

<認定情報・付加情報>

【提出日】	平成15年 2月26日
-------	-------------

次頁無

特願 2 0 0 3 - 0 4 9 7 1 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社